UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608

7590 10/01/2008

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/505,951	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,7-14 and 16-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7-14 and 16-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 22 August 2008 has been entered.

2. By the above submission, Claim 1 has been amended. No claims have been added or canceled. Claims 1, 2, 4, 5, 7-14, and 16-20 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

4. The Examiner notes that Applicant's arguments generally fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. In particular, Applicant alleges that

none of the previously relied upon references discloses the claimed subject matter, but provides no evidence in support of such allegation (see page 6 of the present response).

It is further noted that the features upon which applicant relies (i.e., authenticating consumable state data, see page 6 of the present response) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, the Examiner notes that Applicant has, as in previous actions, argued independent Claims 1 and 11 together, and has more specifically referred to Claim 11 as a dependent claim (see page 6 of the present response). However, although Claim 11 refers to Claim 1, Claim 11 is nevertheless considered to be an independent claim because Claim 11 is directed to a different statutory class of invention (system, i.e. article of manufacture, as opposed to the method of Claim 1) and does not require or explicitly incorporate all of the specific limitations of Claim 1.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 4, 5, 7-14, and 16-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carmon et al, WIPO Publication WO99/10180, in view of Sony Corporation (Kusakabe), European Patent EP 0817420, Spies et al, US Patent 5689565, Atalla et al, US Patent 5319710, and Schneier, *Applied Crypgtography*.

In reference to Claim 1, Carmon discloses a validation protocol for determining authenticity of a printer consumable (page 4, line 20-page 5, line 10) including the steps of providing a printer containing a first authentication chip and a printer consumable containing an second authentication chip (page 11, line 20-page 12, line 2); generating and encrypting a random number in the first authentication chip (page 12, lines 8-12); encrypting the random number in the second authentication chip (page 12, lines 9-11); and comparing the two encrypted random numbers, where if the two encrypted numbers match, then the second chip is considered to be valid and use of the consumable is authorized, or else the second chip is considered to be invalid and use of the consumable is denied (page 12, lines 13-15; see also page 11, lines 10-12). However, Carmon does not explicitly disclose encryption with two different keys.

Sony discloses an authentication method (see Figures 7- 9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated by a random function (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines

41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). Therefore, it would have been obvious to modify the protocol of Carmon to use the specifics of the method taught by Sony, in order to authenticate an untrusted device as an authorized party for communication (see Sony, column 10, lines 31-35; column 14, lines 12-15; see also column 1, line 57-column 2, line 48).

Further, neither Carmon nor Sony discloses the calculation and comparison of a digital signature as a step of the authentication method. Spies discloses a cryptographic system and method that includes generating a digital signature of a document (column 12, lines 6-13) and encrypting the document and digital signature under the same symmetric encryption key in a sending device (column 12, lines 14-27, noting especially the equation at line 25). Spies further discloses decrypting the document and signature at a receiving device (column 13, lines 15-22) and verifying the signature (column 13, lines 20-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Carmon and Sony by including the steps of generating a digital signature of the random number (the “document”) and encrypting the signature with the random number in the first apparatus, and of decrypting and verifying the signature in the second apparatus, in

order to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

Additionally, although Carmon, Sony, and Spies disclose encrypting the random number in the second chip and comparing the encrypted number with the number encrypted in the first chip (as above, at least Sony, column 9, lines 41-48; column 9, line 57-column 10, line 2; and column 10, lines 21-39), none of Sony, Carmon, and Spies explicitly discloses encrypting the decrypted random number along with a memory vector of the second chip. Atalla discloses a method in which, as part of an authentication procedure, a random number is encrypted along with a memory vector in order to produce a number that is sent along with the memory vector to the other device to compare the encrypted numbers to authenticate the message and the first device (see Abstract; column 2, lines 10-34, where the message, sequence number, and PIN are all considered to correspond to the claimed memory vector as broadly described in the present specification). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Carmon, Sony, and Spies by including a memory vector in with the last encryption and comparison steps, in order to further facilitate secure and proper validation (see Atalla, column 2, lines 20-21) and combining the verification of the entity with authentication of the message (see Atalla, title, for example).

Still further, although Carmon, Sony, and Spies disclose that the random number is randomly generated (inherently) and the keys are generated randomly (see, for

example, Spies, column 17, lines 59-61), none of Carmon, Sony, and Spies explicitly discloses that the random function uses a seed to generate the random number. Schneier discloses that good keys should be generated using cryptographically secure pseudo-random-bit generator or a reliably random source (page 173, "Random Keys"). It is further well-known in the art that a linear feedback shift register, which takes a seed, is an example of a type of cryptographically secure pseudo-random-bit generator, and that the seed should be advanced periodically to increase security (Schneier, pages 372-379). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Carmon, Sony, Spies, and Atalla by including the generation of random numbers from a random generator using a seed, in order to realize the predictable result of increasing security by having results generated by an LFSR that are sufficiently random (see Schneier, page 373, third full paragraph; page 173).

In reference to Claim 2, Carmon as modified above further discloses that the first and second keys are held in both the first and second chips (see Sony, Figure 9).

In reference to Claim 4, Carmon as modified above further discloses that the second chip holds a decryption function (see Sony, column 9, lines 31-37).

In reference to Claim 5, Carmon as modified above further discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (Schneier, page 38, last paragraph).

In reference to Claim 7, Carmon as modified above further discloses that the second chip monitors the time elapsed between steps of its processing (see Sony, column 10, lines 53-56).

In reference to Claim 8, Carmon as modified above further discloses that the test function generating the random numbers is held in the first chip (see Sony, column 8, lines 12-15). Additionally, Carmon as modified above discloses that if the second chip is not authenticated, the authentication process is terminated (Sony, column 10, lines 36-39).

In reference to Claim 9, Carmon as modified above further discloses that the first chip monitors the time elapsed between steps of its processing (see Sony, column 10, lines 6-7).

In reference to Claim 10, Carmon as modified above further discloses that it is determined if the second chip is valid (Carmon, page 12, lines 13-15; see also Sony, column 10, lines 31-35) or not (Carmon, page 12, lines 13-15, and page 11, lines 10-12; Sony, column 10, lines 36-39).

In reference to Claim 11, Carmon as modified above generally discloses a system for performing the method of Claim 1 (described above in detail). Carmon as modified above more specifically discloses a printer containing a first authentication chip and a printer consumable containing a second authentication chip (see Carmon, page 4, line 20-page 5, line 10) and that the chips variously include a random number generator, encryption functions and keys for those functions, signature functions, a

prove function that decrypts a random number and signature encrypted using the first key by the first chip and calculates a signature to compare with the received signature, and a test function that generates an encrypted version of a random number and compares the encrypted random number with the received random number (see above, noting the various functions cited in reference to Carmon, for the general authentication using encrypted random numbers, Sony, for the use of two keys and more specifics of the protocol, and Spies, for the incorporation of signatures, and Schneier, for the specifics of the random generating function).

In reference to Claims 12 and 13, Carmon as modified above further discloses that the first chip is a physical authentication chip and that the chips have the same structure (see Carmon, page 11, line 20-page 12, line 2).

In reference to Claim 14, Carmon as modified above further discloses keeping the keys secret (see Sony, column 1, lines 29-41, where symmetric keys are used, and this inherently includes keeping the keys secret to maintain security; see also Figure 9).

In reference to Claim 16, Carmon as modified above further discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (Schneier, page 38, last paragraph).

In reference to Claim 17, Carmon as modified above further discloses that the second chip monitors the time elapsed between steps of its processing (see Sony, column 10, lines 53-56).

In reference to Claim 18, Carmon as modified above further discloses advancing the random number (Schneier, pages 372-379, where LFSRs are advanced as necessary).

In reference to Claim 19, Carmon as modified above further discloses that the first chip monitors the time elapsed between steps of its processing (see Sony, column 10, lines 6-7).

In reference to Claim 20, Carmon as modified above further discloses that it is determined if the second chip is valid (Carmon, page 12, lines 13-15; see also Sony, column 10, lines 31-35) or not (Carmon, page 12, lines 13-15, and page 11, lines 10-12; Sony, column 10, lines 36-39).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. It is noted that Menezes et al, *Handbook of Applied Cryptography*, previously cited by the Examiner and Applicant, generally discloses authentication protocols in which random numbers and other data from memory (e.g. identifiers) are encrypted together.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2137